(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 162 843 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
12.12.2001 Bulletin 2001/50

(51) Int Cl.[7]: **H04N 7/167**

(21) Numéro de dépôt: **01401440.1**

(22) Date de dépôt: **01.06.2001**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **06.06.2000 FR 0007256**

(71) Demandeur: **SAGEM S.A.**
75015 Paris (FR)

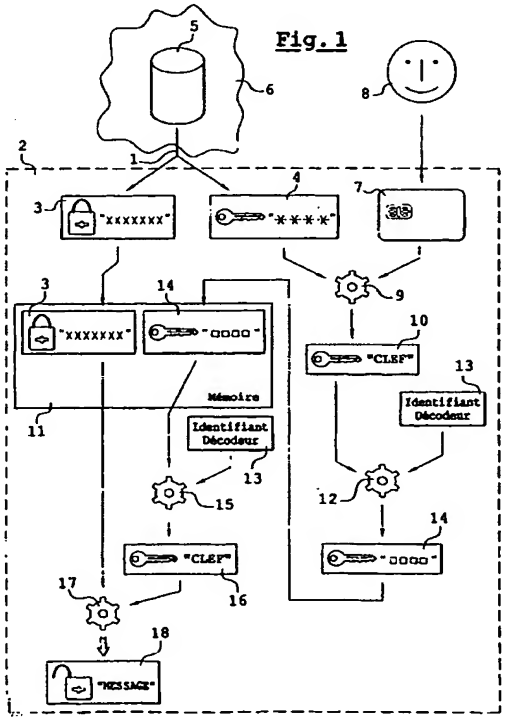
(72) Inventeurs:
- **Cummings, M. John**
  78600 Maisons-Laffitte (FR)
- **Mortreux, M. Bruno**
  76530 Les Essarts (FR)

(74) Mandataire: **Schmit, Christian Norbert Marie**
Cabinet Christian Schmit et Associes,
8, place du Ponceau
95000 Cergy (FR)

(54) Procédé d'enregistrement sécurisé dans un décodeur de télévision

(57) Pour enregistrer un message (3) embrouillé dans un décodeur (2) de télévision à l'aide d'une clé (10) afin d'y accéder à une date différée on enregistre le message embrouillé dans une mémoire (11) du décodeur et on chiffre la clé en utilisant des paramètres (13) d'identification uniques du décodeur. Ainsi, le message embrouillé ne pourra être accessible qu'avec le décodeur qui a permis de chiffrer la clé permettant de désembrouiller le message ainsi enregistré. On peut ainsi visualiser en clair et donc enregistrer un message embrouillé en ayant les droits d'accès à ce message et le regarder à une date ultérieure même si on n'a plus les droits d'accès, la date ultérieure arrivant par exemple après une date limite de validité de ces droits.

Fig. 1



EP 1 162 843 A1

Description

[0001] La présente invention a pour objet un procédé d'enregistrement sécurisé dans un décodeur de télévision. Elle s'applique au domaine de l'audiovisuel par réseau câblé ou par faisceau hertzien voire par satellite. Le but de l'invention est de permettre d'enregistrer des messages à visualiser en temps différé dans le décodeur de télévision tout en s'assurant que le décodeur qui enregistre ce message est bien un décodeur autorisé à le faire.

[0002] Cette invention s'applique plus particulièrement aux messages dont un accès est limité, c'est à dire qu'en fait ils sont embrouillés.

[0003] Actuellement, il est connu d'émettre des messages dont un accès est limité. Pour cela, un opérateur auquel le décodeur de télévision est relié émet des messages embrouillés. Afin de pouvoir désembrouiller le message, il est nécessaire qu'un utilisateur du décodeur considéré soit muni d'un moyen d'authentification lui donnant accès à ces messages embrouillés. Généralement, ce moyen d'authentification est une carte à puce que l'on insère dans un lecteur de carte à puce placé dans le décodeur de télévision. Ainsi, lorsque cette carte à puce est présente dans le lecteur alors celle-ci permet de déchiffrer la clé qui est émise en même temps que le message embrouillé et ce de manière chiffrée. Un utilisateur non muni de cette carte à puce ne pourra pas déchiffrer la clé et donc désembrouiller le message.

[0004] Cet état de la technique fait apparaître un problème de sécurité lié à l'enregistrement de tels messages embrouillés. En effet, lorsqu'un utilisateur souhaite recevoir un message embrouillé pendant son absence pour pouvoir le visualiser en temps différé, c'est à dire à une date ultérieure, il existe alors une première solution qui consiste à enregistrer le message embrouillé en clair c'est à dire de façon désembrouillée. Cette première solution n'est pas très efficace car tout tiers peut avoir accès à ce message en clair. Une deuxième solution consiste à enregistrer le message de manière embrouillée dans une mémoire de sauvegarde ainsi que la clé chiffrée qui l'accompagne. Cette deuxième solution, plus efficace, présente toutefois un problème c'est que certaines cartes à puce sont à accès limité dans le temps. Ainsi il se peut que lorsque l'utilisateur voudra visualiser le message embrouillé qu'il a enregistré il n'aura plus de droits d'accès à ce message puisque sa carte sera arrivée au terme de sa validité. Il ne pourra donc pas visualiser le message embrouillé pour lequel il avait accès lors de sa diffusion puisque la date à laquelle le message est visualisé est une date postérieure à la date limite de validité de la carte à puce.

[0005] La présente invention a pour objet de remédier à ce problème en proposant un moyen d'enregistrement sécurisé, c'est à dire sans que des tiers puissent y avoir accès s'ils n'y sont pas autorisés. Pour cela, on enregistre le message embrouillé dans une mémoire du décodeur de télévision tout en générant une clé chiffrée mais dont un chiffrement est indépendant des caractéristiques de la carte à puce. En outre et selon une caractéristique essentiel de l'invention, on assure que seul le décodeur qui a permis de générer la clé chiffrée pourra lire en clair le message embrouillé placé dans la mémoire de sauvegarde.

[0006] La présente invention a donc pour objet un procédé d'enregistrement sécurisé, dans une mémoire de sauvegarde d'un décodeur de télévision, d'un message reçu par le décodeur et embrouillé par une première clé, caractérisé en ce que la première clé est chiffrée par un moyen de chiffrement du décodeur et enregistrée dans la mémoire de sauvegarde du décodeur avec le message embrouillé.

[0007] La présente invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont présentées qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent :

Figure 1 : un synoptique illustré montrant un fonctionnement du procédé de l'invention.
Figure 2 : un exemple simplifié d'une architecture de décodeur permettant de mettre en oeuvre le procédé de l'invention.

[0008] La figure 1 montre donc un synoptique illustré montrant un fonctionnement du procédé de l'invention. Ce synoptique, dans un souci de clarté, ne fait apparaître que les éléments principaux utiles au procédé de l'invention.

[0009] Ainsi dans une première phase, un décodeur 2 reçoit un message 3 embrouillé que l'on symbolise par la suite "xxxxxxx" ainsi qu'une clé 4 chiffrée que l'on symbolise par la suite "*****". Le message 3 et la clé 4 sont émis à partir d'un serveur 5 de messages dans un réseau 6 de vidéo communication et au travers d'une liaison 1. La liaison 1 entre le serveur 5 et le décodeur 2 peut être un réseau câblé, une liaison hertzienne ou encore une liaison satellite ou tout autre support de communication. Ainsi, pour pouvoir visualiser le message 3 sous une forme désembrouillée, il est tout d'abord nécessaire de déchiffrer la clé 4. Pour cela, on utilise généralement une carte 7 à puce. Cette carte 7 permet d'identifier un utilisateur 8 ou plutôt de donner un accès à l'utilisateur 8 au message 3.

[0010] Dans ce but, on utilise un moyen 9 de déchiffrement généralement présent dans la carte 7. Ainsi, la clé 4 est envoyée au moyen 9 de la carte 7, pendant une phase 2, pour y être déchiffrée. Suite à cette phase 2 la carte 7 émet alors une clé 10 correspondant à la version déchiffrée de la clé 4 que l'on peut alors symboliser par la suite "CLEF". C'est cette clé 10 qui permet de désembrouiller le message 3 et afin de pouvoir le visualiser dans de bonnes conditions.

[0011] Dans l'invention, l'utilisateur 8 souhaite enregistrer le message 3 dans une mémoire 11 de sauvegarde afin de pouvoir le visualiser en temps différé par

rapport à une date d'émission par le serveur 5. Ainsi, selon une caractéristique essentielle de l'invention, le décodeur 2 coopère avec un moyen 12 de chiffrement pour chiffrer la clé 10. Dans un exemple de mise en oeuvre du procédé la clé 10 est envoyée au moyen 12. En outre, le moyen 12 utilise un moyen 13 d'identification du décodeur 2 pour chiffrer la clé 10. Ce moyen 13 peut être un identifiant du décodeur tel qu'un numéro de série unique par exemple. Ce moyen 13 peut aussi très bien être un numéro secret quelconque et unique, chaque numéro étant alors associé à un seul décodeur. Cependant, on considérera, à titre d'exemple, que le moyen 13 correspond au numéro de série du décodeur 2.

[0012] En conséquence, on génère, dans une phase 3, une clé 14 chiffrée mais différente de la clé 4 pouvant être représenté par la suite " ". Ainsi, cette clé 14 est associée au décodeur 2 et non pas avec la carte 7 comme pour la clé 4.

[0013] Dans une phase 4, on mémorise la clé 14. A cet instant, la mémoire 11 comporte le message 3 embrouillé et la clé 14 correspondant à la clé 10 mais chiffrée en utilisant le moyen 13 d'identification du décodeur 2.

[0014] Lorsque l'utilisateur 8 veut visualiser le message 3 présent dans la mémoire 11, il faut tout d'abord déchiffrer la clé 14, lors d'une phase 5 de déchiffrement, pour passer de la suite " ", correspondant à la clé 14, à la suite "CLEF" afin d'autoriser une visualisation de ce message 3. Pour cela, on lit une valeur de la clé 14 dans la mémoire 11 et on l'envoie à un moyen 15 de déchiffrement. Ce moyen 15 utilise en outre le moyen 13 d'identification du décodeur 2 c'est à dire par exemple le numéro de série. Cela permet de vérifier que l'on est bien dans le même décodeur qui a permis le chiffrement de la clé 10. Ainsi, on obtient une clé 16 identique à la clé 10 que l'on va ainsi représenter aussi par la suite "CLEF".

[0015] Dans une phase 6 de désembrouillage, on envoie le message 3 à un moyen 17 de désembrouillage qui permet d'obtenir un message 18 correspondant à la version en clair du message 3, pouvant alors être représenté par la suite "MESSAGE". Il faut cependant que la clé 16 corresponde bien à la clé 10, laquelle clé 16 est évidemment envoyée au moyen 17 et utilisée par ce dernier.

[0016] Dans un exemple préféré de mise en oeuvre du procédé de l'invention, c'est le décodeur 2 qui est muni des moyens 12 et 15 pouvant se présenter sous la forme de programmes de chiffrement et de déchiffrement des clés 10 et 14 respectivement. Ainsi, la carte 7 ne sera utilisée qu'une seule fois afin de servir de contrôleur d'accès au message 3 embrouillé. Cette phase de contrôle d'accès aura lieu par exemple lors de la phase d'enregistrement à la date de diffusion de ce message 3. En effet, si la carte 7 n'autorise pas un accès de l'utilisateur 8 au message 3 alors les phases 3, 4, 5 et 6 n'auront pas lieu d'être mises en oeuvre puisque il n'y a pas la possibilité de visualiser en clair le message 3 à la date de diffusion.

[0017] La figure 2 montre un exemple simplifié d'une architecture du décodeur 2 permettant de mettre en oeuvre le procédé de l'invention. Ainsi, le décodeur 2 est donc relié d'une part au serveur 5 du réseau 6 par la liaison 1 et d'autre part à un téléviseur 19. Le décodeur 2 comporte principalement un dispositif 20 de réception relié à la liaison 1 et recevant donc des messages tels que le message 3 embrouillé et la clé 4 correspondant à la clé 10 chiffrée par exemple par l'opérateur du réseau 6 ou par le producteur du message 3 embrouillé. Le décodeur 2 comporte en outre la mémoire 11 de la figure 1, un microprocesseur 21 commandé notamment par les moyens 12 et 15 (figure 1) présents dans une mémoire 22 de programme sous forme de programmes de chiffrement et de déchiffrement respectivement. En outre, le décodeur 2 comporte un lecteur 23 de carte à puce permettant de coopérer avec la carte 7. Ainsi, le message 3 et la clé 4 sont reçus par le récepteur 20 puis la clé 4 est envoyée par le microprocesseur 21 à la carte 7 afin d'y être traitée. La carte 7 renvoie alors au microprocesseur 21 la clé 4 (figure 1) déchiffrée.

[0018] Le programme 12 dans la mémoire 22 commande en conséquence le microprocesseur 21 afin de produire la clé 14 et de la sauvegarder dans la mémoire 11 avec le message 3 embrouillé. Le programme 15 de la mémoire 22 permet quant à lui de déchiffrer la clé 14. Une fois la clé 14 déchiffrée c'est à dire une fois la clé 16 obtenue (figure 1), cette dernière est envoyée au moyen 17 prenant généralement la forme, dans le décodeur 2, d'un circuit intégré dédié à la fonction de désembrouillage. Puis, le message 3 est envoyé au moyen 17 qui peut désembrouiller le message 3 afin d'en obtenir une version dite en clair. Cette version en clair est envoyée par exemple à un moyen 24 de gestion vidéo. Ce moyen 24 a en charge de traiter les signaux produits par le moyen 17 et de les mettre sous une forme utilisable par le téléviseur 19 généralement des signaux analogiques ou même un signal vidéo composite.

[0019] Bien évidemment, les éléments du décodeur 2 sont reliés entre eux par un bus 25 afin de permettre une communication entre ces différents éléments et ce généralement sous le contrôle du microprocesseur 21 commandé par un programme 26 de gestion du décodeur de la mémoire 22.

[0020] On a vu que dans un exemple préféré les moyens 12 et 15 étaient présents dans le décodeur et gérés par le décodeur. Cependant, dans une variante, on peut envisager de placer les moyens 12 et 15 dans une carte à puce telle que la carte 7 par exemple. La carte 7 aurait alors la charge de passer de la clé 4 à la clé 14 comme précédemment. Dans ce cas, le microprocesseur 21 envoie à la carte 7, dans cet exemple, l'identifiant du décodeur 2 et donc plus généralement le moyen 13. On peut aussi envisager de munir le décodeur 2 d'un composant de sécurité sous forme d'un circuit intégré notamment. Ce composant permettrait de

mettre en oeuvre les moyens 12 et 15 dans un environnement sécurisé comme dans une carte à puce.

[0021] En outre, le moyen 13 d'identification du décodeur peut être un numéro de série mémorisé dans la mémoire 11 à un emplacement 27. Dans une variante, on limite un accès au moyen 13 par exemple en chiffrant le numéro de série mémorisé à l'emplacement 27 par un programme de chiffrage et déchiffrage présent dans la mémoire 22 de programme par exemple.

[0022] Un programme de chiffrement et ou de déchiffrement utilisé pour les moyens 12 et 15 est fonction en fait de la complexité et du niveau de sécurité recherché pour cet enregistrement sécurisé. En effet, de manière la plus simple possible un programme de base pourra être une opération logique de type OU-EXCLUSIF entre le numéro de série et la valeur de la clé 10. Bien sûr, il est possible d'utiliser des algorithmes beaucoup plus évolués et parfaitement connus du domaine de la cryptologie.

[0023] Dans une variante, on produit un message composite à chiffrer en réalisant une concaténation entre la valeur de la clé 10 et la valeur de l'identifiant du décodeur 2 par exemple son numéro de série. Ainsi, et selon un exemple de réalisation, on réalise cette concaténation entre une valeur chiffrée, par un programme de chiffrement (non représenté), du numéro de série et la valeur de la clé 10 afin de ne pas avoir dans la clé 14 une faille de sécurité. En effet, si on utilisait la valeur du numéro de série en clair et que celle-ci est accessible pour une raison ou pour une autre alors la clé 14 résultante sera d'un très faible niveau de sécurité puisqu'une partie du message est parfaitement connue. En outre, le fait de placer ce programme de chiffrement déchiffrement dans une carte à puce renforce encore la sécurité de cette réalisation.

[0024] Par contre, le chiffrement de la valeur du numéro de série implique, pour les mêmes raisons, que l'on ne sauvegarde pas cette valeur chiffrée dans un endroit accessible. D'ailleurs, il y a peu d'intérêt à sauvegarder la valeur chiffrée du numéro de série puisqu'il suffira de tout d'abord déchiffrer la clé 14 puis de déchiffrer le numéro de série chiffré ainsi obtenu et de comparer cette valeur déchiffrée avec le numéro de série mémorisé à l'emplacement 27. Si ces deux informations sont égales alors le message 3 pourra être désembrouillé par le moyen 17.

Revendications

1. Procédé d'enregistrement sécurisé, dans une mémoire (11) de sauvegarde d'un décodeur (2) de télévision, d'un message (3) reçu par le décodeur et embrouillé par une première clé (10), **caractérisé en ce que** la première clé est chiffrée par un moyen (12) de chiffrement du décodeur et enregistrée dans la mémoire de sauvegarde du décodeur avec le message embrouillé.

2. Procédé selon la revendication 1 **caractérisé en ce que** on chiffre la première clé en utilisant un moyen (13) d'identification du décodeur.

3. Procédé selon la revendication 2 **caractérisé en ce que** le moyen d'identification est un identifiant du décodeur.

4. Procédé selon la revendication 3 **caractérisé en ce que** :

   - on chiffre l'identifiant,
   - on réalise une concaténation entre l'identifiant et la première clé à chiffrer.

5. Procédé selon l'une des revendications 1 à 4 **caractérisé en ce que** on autorise une visualisation du message embrouillé par déchiffrement de la première clé chiffrée en utilisant le moyen d'identification du décodeur.

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel la première clé est reçue codée par le décodeur, **caractérisé en ce que** ladite première clé est décodée par le décodeur avant d'être chiffrée par le moyen de chiffrement (12).

7. Procédé selon l'une des revendications 1 à 6 **caractérisé en ce que** on munit le décodeur d'un programme de chiffrement et ou déchiffrement de la première clé ou d'une deuxième clé.

8. Procédé selon l'une des revendications 1 à 7 **caractérisé en ce que** on munit le décodeur d'un lecteur de carte à puce recevant une carte (7) à puce d'authentification d'un utilisateur (8) du décodeur, et **en ce que** on chiffre la première clé dans la carte à puce.

Fig. 1

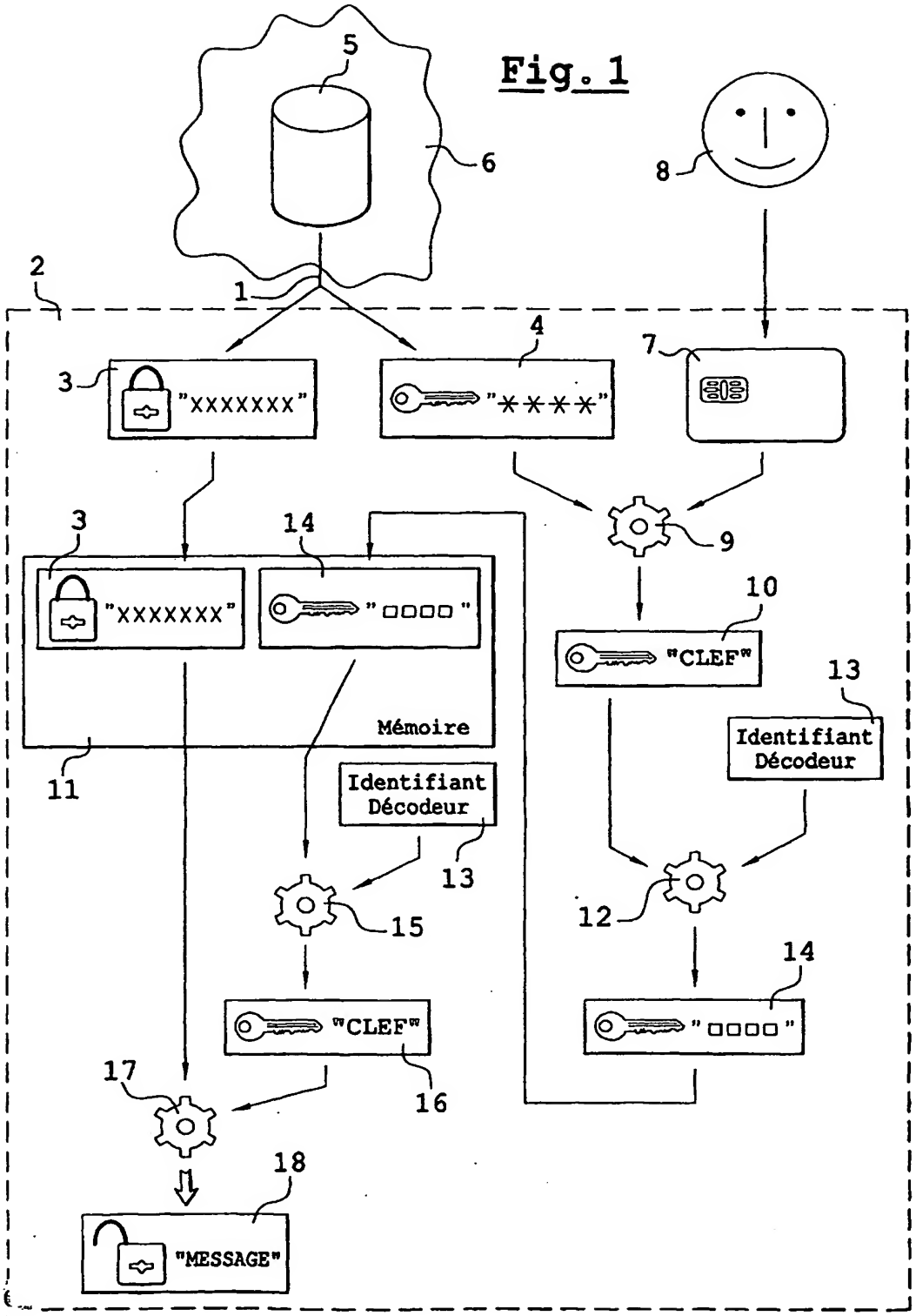
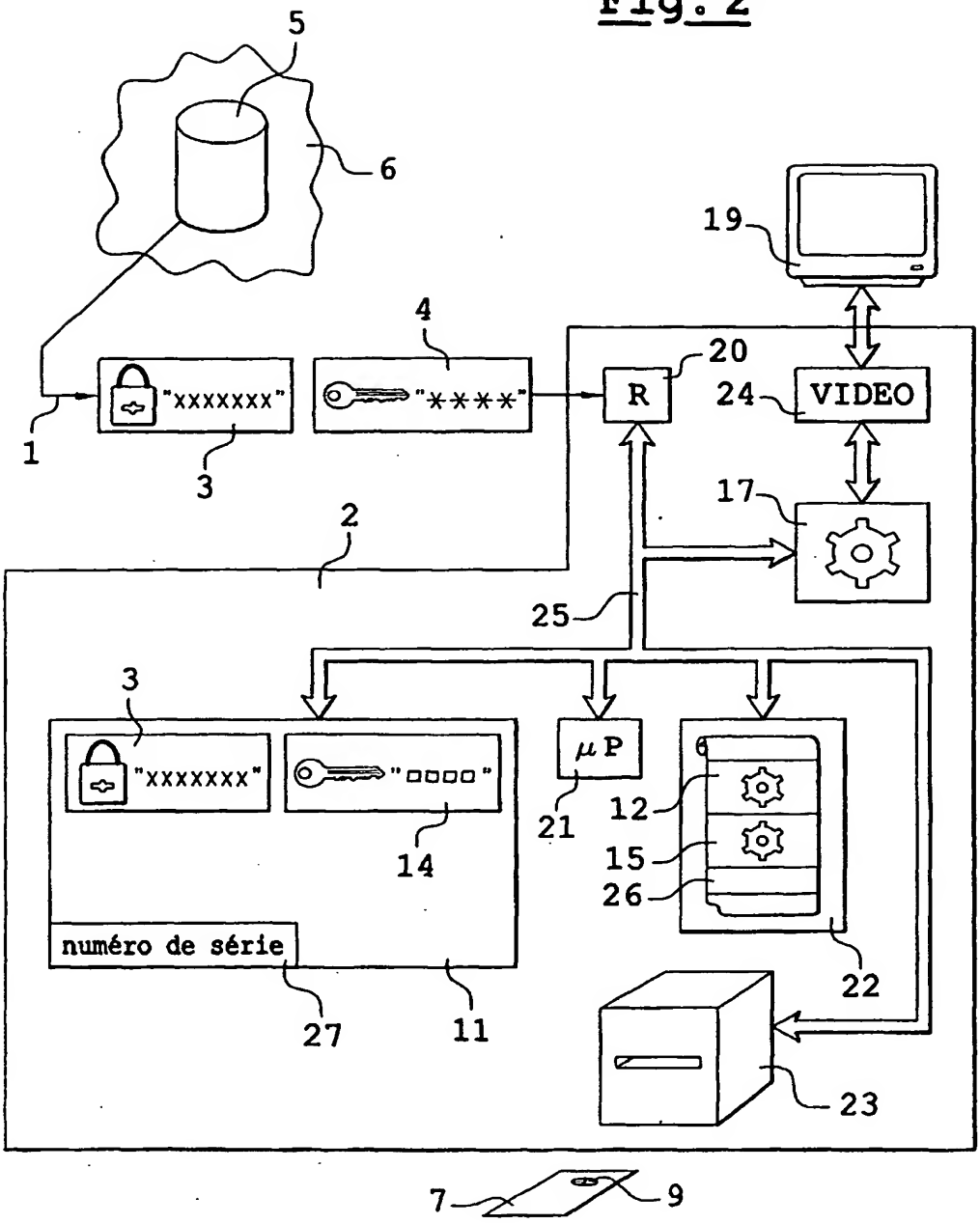

5
6
8
2
1
4
7
3
"XXXXXXX"
"****"
9
3
14
"XXXXXXX"
"□□□□"
10
"CLEF"
13
Identifiant Décodeur
Mémoire
11
Identifiant Décodeur
13
15
12
14
"CLEF"
"□□□□"
17
16
18
"MESSAGE"

Fig. 2


5
6
19
4
20
"xxxxxxx"
"****"
R
24
VIDEO
1
3
17
2
25
3
"xxxxxxx"
"□□□□"
μP
21
12
15
26
14
numéro de série
22
27
11
23
7
9

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 01 40 1440

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X A	EP 0 858 184 A (NDS LTD) 12 août 1998 (1998-08-12) * colonne 2 - colonne 7, ligne 20 * * colonne 10, ligne 14 - ligne 19 * * figures 2,4 *	1-3,5-8 4	H04N7/167
X A	WO 00 04718 A (BENARDEAU CHRISTIAN ;CANAL PLUS SA (FR); DAUVOIS JEAN LUC (FR)) 27 janvier 2000 (2000-01-27) * page 2, ligne 25 - page 3, ligne 9 *	1,2,5 3,4,6-8	
A	US 5 237 610 A (GAMMIE KEITH ET AL) 17 août 1993 (1993-08-17) * le document en entier *	1-8	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)
H04N

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	25 septembre 2001	Tito Martins, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 01 40 1440

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

25-09-2001

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0858184	A	12-08-1998	IL	120174 A	28-10-1999
			EP	0858184 A2	12-08-1998
			US	6178242 B1	23-01-2001
			GB	2322030 A ,B	12-08-1998
WO 0004718	A	27-01-2000	AU	4642599 A	07-02-2000
			BR	9912091 A	03-04-2001
			EP	1099348 A1	16-05-2001
			WO	0004718 A1	27-01-2000
			NO	20010227 A	15-03-2001
US 5237610	A	17-08-1993	US	5029207 A	02-07-1991
			AT	144670 T	15-11-1996
			AT	181196 T	15-06-1999
			AT	180373 T	15-06-1999
			AU	650958 B2	07-07-1994
			AU	1384092 A	01-10-1992
			BR	9201106 A	24-11-1992
			CN	1066950 A ,B	09-12-1992
			DE	69214698 D1	28-11-1996
			DE	69214698 T2	06-03-1997
			DE	69229235 D1	24-06-1999
			DE	69229235 T2	23-09-1999
			DE	69229408 D1	15-07-1999
			DE	69229408 T2	11-11-1999
			EP	0506435 A2	30-09-1992
			EP	0679029 A1	25-10-1995
			EP	0683614 A1	22-11-1995
			JP	5145923 A	11-06-1993
			SG	44801 A1	19-12-1997
			AT	180936 T	15-06-1999
			AT	192891 T	15-05-2000
			AU	635180 B2	11-03-1993
			AU	7340291 A	21-08-1991
			BR	9104261 A	03-03-1992
			CA	2049310 A1	02-08-1991
			DE	69131285 D1	08-07-1999
			DE	69131285 T2	30-09-1999
			DE	69132198 D1	15-06-2000
			DE	69132198 T2	23-11-2000
			EP	0466916 A1	22-01-1992
			EP	0809402 A1	26-11-1997
			JP	4506736 T	19-11-1992
			MX	172416 B	15-12-1993
			WO	9111884 A1	08-08-1991

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

European Patent Office

EP 1 162 843 A1

APPLICATION FOR A EUROPEAN PATENT

Publication Date:
12.12.2001
Registration No.: **01401440.1**
Registration Date: **01.06.2001**

Int. Cl.[7]: **H04N 7/167**

Convention Signatories Designated:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Extension Countries Designated:
AL LT LV MK RO SI

Priority: 06.06.2000 FR 0007256

Applicant: **SAGEM S.A.**
75015 Paris (FR)

Inventors:
- Cummings, M. John
  78600 Maisons-Laffitte (FR)
- Mortraux, M. Bruno
  76530 Les Esserts (FR)

Represented by: **Schmit, Christian Norbert Ma**
Cabinet Christian Schmit et Associes,
8 place du Ponceau
95000 Cergy (FR)

Procedure of Secure Recording in a television decoder

In order to record a scrambled transmission (3) in a television decoder (2) with the help of a key (10) so as to have access to it on another date, the scrambled transmission is recorded in the decoder memory (11) and the key is coded using the unique identification parameters (13) of the decoder. Moreover, the scrambled transmission can only be accessed by the decoder by means of which the key was coded, thus permitting the unscrambling of the recorded transmission. It is also possible to view and hence to record an unscrambled transmission if one possesses access authorization to that transmission, which may be viewed on a later date when the access authorization has expired, e.g. if the later viewing date occurs after the date of termination of the validity of such authorization.

Description

[0001] The present invention provides a secure recording procedure by a television decoder. The procedure may be applied to cable television or to a beam transmission, including by satellite. The aim of the invention is to enable recording transmissions in the television decoder to be viewed at some other time, making sure that the decoder recording the transmission is indeed authorized to carry out such operation.

[0002] The invention is applicable in particular to limited access transmissions, i.e. scrambled transmissions.

[0003] Limited access transmissions are common today. To that end, an operator with whom the television decoder is associated broadcasts the scrambled transmission. In order to unscramble the transmission it is necessary for the user of the decoder to be equipped with an authenticating means as one having access to such scrambled transmissions. Generally, this authenticating means is a chip card inserted into a chip-card reader contained in the television decoder. Since that chip card is located within the card reader, it enables decoding the key transmitted concurrently with the scrambled message, in coded form. A user not equipped with that chip card can not decode the key and is thus unable to unscramble the transmission.

[0004] That state of the art gives rise to a security problem related to the recording of such scrambled transmissions. In effect, when the user wants to receive a scrambled transmission in his absence in order to view it at some other time, i.e. later on, one solution is to record the scrambled transmission in unscrambled form. This solution is not very effective since any third party will have access to the unscrambled transmission. A second solution is to record the scrambled transmission in a buffer memory together with the coded key which accompanies it. This second solution, which is more efficacious, involves however a problem in that certain chip cards are only valid for a limited period of time. It may thus turn out that when the user wishes to view the scrambled transmission which he has recorded, he will no longer be authorized to have access to that transmission since the validity of his card has expired. He will therefore not be able to view the scrambled transmission to which he had access at the time it was broadcast, because the viewing date of that transmission occurs later than the terminal date of validity of the chip card.

[0005] The present invention aims to resolve this problem by offering a means of secure recording, i.e. denying access to third parties if they are unauthorized. To that end the scrambled transmission is recorded in a memory contained in the television

decoder along with a generated coded key, but this coding is independent of the characteristics of the chip card. Moreover, and this an essential characteristic of the invention, the method assures that only the decoder allowed to generate the coded key can read out the scrambled transmission recorded in the buffer memory.

[0006] The invention proposes a secure recording procedure in a buffer memory contained in the television decoder, whereby a transmission received by the decoder which has been scrambled using a first key is characterized is that the first key is coded by a coding means contained in the decoder and is recorded in the decoder buffer memory together with the scrambled transmission.

[0007] The invention will now be described in more detail by relating to the attached drawings. These drawings are provided for the sake of illustration only and do not limit the invention in any way. The figures show:

Figure 1: a block diagram illustrating the functioning of the procedure according to the invention.

Figure 2: a simplified example of the architecture of the decoder permitting to carry out the procedure according to the invention.

[0008] Figure 1 is a block diagram illustrating the functioning of the procedure according to the invention. In the interests of clarity, only the chief components employed in the procedure are shown.

[0009] At first, the decoder 2 receives the scrambled transmission 3 symbolically indicated by the sequence "xxxxxxx" as well as a 4 digit key symbolically indicated by the sequence "****". The transmission 3 and the key 4 are transmitted by the server 5 of a video network 6 through the link 1. The link 1 between the server 5 and the decoder 2 may be a cable network, a free beam or a satellite link, or indeed any other communication medium. In order to be able to view the transmission 3 in unscrambled form, it is first necessary to decode the key 4. This is generally done by the chip card 7. This card 7 permits the identification of the user 8 so as to grant this user access to the transmission 3.

[0010] To that end use is made of the decoding means 9 generally included in the card 7. The key 4 is transmitted to the means 9 of the card 7 in the second stage, to be decoded. At the end of that stage the card 7 puts out a key 10 corresponding to the decoded version of the key 4, which is symbolically labeled "KEY" on the diagram.

That key 10 permits the unscrambling of the transmission 3 and allows to view it properly.

[0011] According to the invention, the user 8 would record the transmission 3 in the buffer memory 11 so as to be able to view it at a different time than that on which it was transmitted by the server 5. Also, according to an essential characteristic of the invention, the decoder 2 cooperates with the coding means 12 in order to encode the key 10. In the example of an embodiment of the procedure, the key 10 is passed over to the means 12. In addition, the means 12 uses an identifying means 13 of the decoder 2 in order to encode the key 10. That means 13 may be an identifier of the decoder, such as a unique serial number, for example. That means 13 may also very well be some unique secret number whereby each such number is associated with a single decoder only. However, in the example presented the means 13 will be considered to correspond to the serial number of the decoder 2.

[0012] In the third stage a coded key 14 is generated, which differs from the key 4, and which is represented by the sequence " ". That key 14 is associated with the decoder 2 and not with the card 7, unlike the key 4.

[0013] In the fourth stage the key 14 is entered into memory. From that point on, the memory 11 contains the scrambled transmission 3 as well as the key 14 corresponding to the key 10 but coded by using the identifying means 13 of the decoder 2.

[0014] When the user 8 wishes to view the transmission 3 contained in the memory 11, he must first decode the key 14, in a fifth stage of decoding, for passing from the sequence " ", corresponding to the key 14 to the sequence "KEY" in order to authorize the viewing of the transmission 3. To that end, one value of the key 14 is read from the memory 11 and the decoding is transferred to the means 15. This means 15 also uses the identifying means 13 of the decoder 2, i.e. the serial number, for example. This permits verification that the process occurs within the same decoder which permits the key 10 to be decoded. In this manner a key 16 is obtained which is identical to the key 10 and which is also represented by "KEY" on the diagram.

[0015] In the sixth stage of the unscrambling process, the transmission 3 is passed over to the unscrambling means 17 from which it comes out as the transmission 18 corresponding to the unscrambled version of the transmission 3, here represented by the word "TRANSMISSION". It is necessary, however, that the key 16 corresponds well to the key 10. This key 16 is evidently sent to the means 17 and put to use in it.

[0016] In a preferred embodiment of the procedure according to the invention, the decoder 2 is equipped with the means 12 and 15 which may be represented in the form

of coding and decoding programs of the keys 10 and 14, respectively. The card 7 is used just once to serve as the access controller of the scrambled transmission 3. This stage of access control will take place, for example at the recording stage at the time of broadcasting of the transmission 3. In effect, if the card 7 does not authorize access of the user 8 to the transmission 3 then the third, fourth, fifth and sixth stages will not take place and it will be impossible to view the unscrambled transmission 3 on the date it is broadcast.

[0017] Figure 2 shows a simplified example of the architecture of the decoder 2, enabling the procedure according to the invention to be carried out. The decoder 2 is linked on one side to the server 5 of the network 6 by the link 1, and on the other side to the television receiver 19. The decoder 2 contains mainly the apparatus 20 for real-time reception through the link 1 and thus receives transmissions such as the scrambled transmission 3 and the key 4 corresponding to the coded key 10, for example, from the operator of the network 6 or from the producer of the scrambled transmission 3. The decoder 2 further contains the memory 11 of Figure 1, a microprocessor 21 controlled mainly by the means 12 and 15 (Figure 1) located in the program memory 22 in the form of coding and decoding programs, respectively. In addition, the decoder 2 contains the reader 23 of the chip card which permits cooperation with the card 7. The transmission 3 and the key 4 are received by the receiver 20 together with the key 4 which is sent by the microprocessor 21 to the card 7 for treatment. The card 7 then returns to the microprocessor 21 the decoded key 4 (Figure 1).

[0018] The program 12 residing in the memory 22 thus controls the microprocessor 21 so as to produce the key 14 and preserve it in the memory 11 along with the scrambled transmission 3. The program 15 residing in the memory 22 permits the decoding of the key 14. Once the key 14 is decoded, i.e. once the key 16 is obtained (Figure 1), that latter is passed over to the means 17 which generally assumes the form, within the decoder 2, of an integrated circuit dedicated to the unscrambling function. Next the transmission 3 is passed over to the means 17 which unscrambles the transmission 3 to obtain a decoded version of it. This decoded version is sent, for example, to a means 24 of video management. That means 24 is in charge of handling the signals produced by the means 17 so as to convert them into a form usable by the television receiver 19, generally as analogic signals or in the form of a composite video signal.

[0019] Evidently, the components of the decoder 2 are all interconnected by the bus 25 enabling communication among the various components under the general control of

the microprocessor 21 governed by the decoder program 26 which manages the memory 22.

[0020] It should be noted that in the preferred example shown, the means 12 and 15 are presented as located in the decoder and managed by the decoder. However, in a variant embodiment, it is possible to locate the means 12 and 15 on a chip card, such as the card 7, for example. The card 7 will then have the task of passing over from the key 4 to the key 14, as aforesaid. In this case, the microprocessor 21 transfers to the card 7, in that example, the identifier of the decoder 2, and more generally the means 13. It is also possible to conceive equipping the decoder 2 with a security component in the form of an integrated circuit. That component would permit the means 12 and 15 to be operated in a secured environment, as within a chip card.

[0021] In addition, the identifying means 13 of the decoder could be a serial number memorized in the memory 11 at the location 27. In a variant embodiment, access to the means 13 is limited, e.g. by coding the serial number stored at location 27 by a coding - decoding program residing in the programming memory 22, for example.

[0022] A coding and/or decoding program used for the means 12 and 15 depends on the complexity and on the security level desired for that secured recording. In effect, the simplest possible basic program would be an EXCLUSIVE-OR logic operation between the serial number and the value of key 10. Certainly it is possible to use more advanced algorithms such as are well known in the field of cryptology.

[0023] In a variant embodiment, a composite transmission is produced by encoding a string consisting of the value of the key 10 and the value of the identifying label of the decoder 2, such as its serial number. However, and indeed according to a realized example, this string consists of a coded value, produced by application of the coding program (not shown on the figures), the serial number of the value of key 10 (in order not to have the value of key 10 contained in that of key 14, which would breach security). In effect, if the serial number is used uncoded and is accessible because of any reason whatever, the resultant key 14 would provide a very low level of security since part of the transmission would be entirely known beforehand. In addition, locating the coding-uncoding program on a chip-card further reinforces security.

[0024] On the other hand, the coding of the value of the serial number implies, for the same reasons, that this coded value is not kept at an accessible location. However, there would be little interest in guarding a coded value of a serial number, because it would be sufficient to decode the key 14 in order to decode the serial number obtained by

comparing this coded value with the serial number memorized at location 27. If these two data are identical, then the transmission 3 may be unscrambled by the means 17.

Claims

1. Secured recording procedure, in a buffer memory (11) of a decoder (2) of a television receiver, of a transmission (3) received by the decoder and scrambled by a first key (10), **characterized in that** the first key is coded by the coding means (12) of the decoder and is recorded in the buffer memory of the decoder together with the scrambled transmission.
2. Procedure according to Claim 1, **characterized in that** the first key is coded by using the identifying means (13) of the decoder.
3. Procedure according to Claim 2, **characterized in that** the identifying means is the identifier of the decoder.
4. Procedure according to Claim 3, **characterized in that**:
   - the identifier is coded,
   - a string is formed consisting of the identifier and the first key to be coded.
5. Procedure according one of the Claims 1 to 4, **characterized in that** viewing of the scrambled transmission is authorized by decoding the first coded key by using the identifying means of the decoder.
6. Procedure according to any of the Claims 1 to 5, whereby the first key is received coded by the decoder, **characterized in that** said first key is decoded by the decoder before being coded by the coding means (12).
7. Procedure according one of the Claims 1 to 6, **characterized in that** the decoder is provided with a coding program and/or decoding of the first key or of the second key.
8. Procedure according to any of the Claims 1 to 7, **characterized in that** the decoder is provided with a chip-card reader receiving a chip-card (7) of authentication of the user (8) of the decoder, and **by means of it** the first key of the chip-card is coded.

Fig. 1

[on the left, top to bottom:]

memory

decoder identifier

"KEY"

"TRANSMISSION"

[on the right:]

"KEY"

decoder identifier

Fig. 2

[on the left]

serial number

European Patent Office

EUROPEAN SEARCH REPORT

Application No.
EP 01 40 1440

DOCUMENTS CONSIDERED PERTINENT			
Category	Document Citation with Indication, if needed, of the pertinent parts	Claim Concerned	Application Class (Int. Cl.7)
X A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) * column 2 – column 7, line 20 * * column 10, line 14 – line 19 * * figures 2, 4 * ---	1-3,5-8 4	
X A	W0 00 04718 A (BENARDEAU CHRISTIAN ; CANAL PLUS SA (FR); DAUVOIS JEAN LUC (FR)) 27 January 2000 (2000-01-27) * page 2, line 25 – page 3; line 9 * ---	1,2,5 3,4,6-8	
A	US 5 237 610 A (GAMMIE KEITH ET AL) 17 August 1993 (1993-08017) * the entire document * ---	1-8	
			Technical Fields searched (int.Cl.7)
			H04N

The present report covers all claims

Place of search	Date of search completion	Examiner
The Hague	25 September 2001	Tito Martins, J

CATEGORY OF DOCUMENTS CITED

X: particularly pertinent in itself
Y: particularly pertinent in combination with another document of the same category
A: prior art
O: verbal communication
F: intermediary document

T: Theory or principle on which the invention is based
E: Prior patent document, but published on the application date or later
D: Cited in the patent application
L: Cited for other [illegible]

.....

&: member of the same family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT RELATIVE TO EUROPEAN PATENT APPLICATION NO. EP 01 40 1440

The present annex indicates members of the patent family related to the patent documents cited in the European search report on the preceding page.

These members are contained in a computer file of the European Patent Office dated:

.....

The information provided is for understanding only and does not involve the responsibility of the European Patent Office.

25-09-2001

Patent Document Cited in the search report	Publication date	Members of the patent family	Publication date
[table, see original.]			

For information concerning this annex, see the Official Gazette of the European Patent Office, No. 12/82.